

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**

Jillian Cantinieri, individually, and on behalf of all others similarly situated, <div style="text-align: center;">Plaintiff, -v- Verisk Analytics, Inc., <i>et al.</i>, Defendants.</div>	2:21-cv-6911 (NJC) (JMW)
--	-----------------------------

OPINION AND ORDER

NUSRAT J. CHOUDHURY, United States District Judge:

Plaintiff Jillian Cantinieri (“Cantinieri”) brings this action on behalf of herself and a putative class of similarly situated individuals against Defendants Verisk Analytics, Inc. (“Verisk Analytics”), Insurance Services Office, Inc. (“Insurance Services Office”), and ISO Claims Services Inc. (“ISO Claims,” and collectively, “Defendants”) for failing to safeguard her personally identifiable information (“PII”) stored in Defendants’ web portal from unauthorized access by other entities or cybercriminals. (Am. Compl. at 1, ECF No. 72.) Before me is Defendants’ fully briefed Motion to Dismiss the Amended Complaint pursuant to Rule 12(b)(1) and (b)(6) of the Federal Rules of Civil Procedure (“Fed. R. Civ. P.”). (ECF No. 79.) For the reasons stated below, Cantinieri lacks Article III standing to pursue her claims. Therefore, Defendants’ Motion to Dismiss is granted and the Amended Complaint is dismissed without prejudice pursuant to Rule 12(b)(1).

FACTUAL BACKGROUND

As discussed in the Legal Standards section below, for the purpose of evaluating Defendants’ Rule 12(b)(1) motion, I accept the Amended Complaint’s factual allegations as true

except where evidence in the record directly contradicts a specific factual allegation; where there is such a contradiction, I consider whether Cantinieri has proven the alleged facts to support standing by a preponderance of the evidence. *See* Legal Standards, *infra*; *Harty v. W. Point Realty, Inc.*, 28 F.4th 435, 442 (2d Cir. 2022); *see also Lugo v. City of Troy*, 114 F.4th 80, 87 (2d Cir. 2024); *Tandon v. Captain’s Cove Marina of Bridgeport, Inc.*, 752 F.3d 239, 243 (2d Cir. 2014); *Katz v. Donna Karan Co.*, 872 F.3d 114, 120 (2d Cir. 2017).¹ I therefore first describe the facts alleged in the Amended Complaint in support of Cantinieri’s claims and then describe the parties’ factual submissions on Defendants’ Rule 12(b)(1) Motion to Dismiss.

I. The Amended Complaint’s Allegations Relating to Standing

Defendants are a corporation and its subsidiaries that “own, operate and maintain databases and web portals” through which Defendants collect, contain, and provide users with access to insurance claim records, motor vehicle records from state Departments of Motor Vehicle (“DMVs”), and the PII of millions of individuals. (Am. Compl. ¶¶ 2, 21, 30, 41.) ISO Claims is a subsidiary of Insurance Services Office, which in turn is a subsidiary of Verisk Analytics. (*Id.* ¶¶ 22–23, 42, 50.) Through their web portals, Defendants acquire and provide access to individuals’ PII, including “full names, addresses, telephone numbers, vehicle identification numbers . . . , license plate numbers, driver’s license numbers, tax identification numbers . . . , and/or Social Security Numbers.” (*Id.* ¶ 3.) Defendants, through their subsidiary, Insurance Information Exchange (“iiX”), operate the ExpressNet portal, which is a web portal

¹ As discussed below, I do not reach Defendants’ Rule 12(b)(6) motion because Cantinieri lacks Article III standing to pursue her claims. If I were to analyze that motion, I would accept all factual allegations in the Amended Complaint as true and draw all reasonable inferences in favor of Cantinieri. *See Melendez v. City of New York*, 16 F.4th 992, 1010 (2d Cir. 2021).

through which customers can obtain motor vehicle records from state DMVs. (*Id.* ¶¶ 4, 49–52.)

As early as July 5, 2021, “unauthorized entities or cybercriminals” used the ExpressNet web portal to access and obtain DMV records for Cantinieri and others. (*Id.* ¶ 4.) These DMV records included Cantinieri’s PII. (*Id.*) The Amended Complaint further alleges “upon information and belief” that, before this “data breach,” Cantinieri’s insurer submitted automobile claim information to Defendants which included Cantinieri’s full name, address, date of birth, driver’s license number, and Social Security Number (“SSN”). (*Id.* ¶ 10.) It also alleges “upon information and belief” that this PII was disclosed to the “unauthorized entities or criminals” as part of the “data breach,” and that the authorized entities or cybercriminals used Cantinieri’s PII to themselves commit identity theft or fraud, or otherwise released or sold her PII to other entities who used her PII to commit identity theft or fraud. (*Id.* ¶¶ 10, 13.)

The Amended Complaint alleges “upon information and belief” that the disclosure of Cantinieri’s PII occurred “much earlier than reported by ISO CLAIMS,” (*id.* ¶ 81)² and that unauthorized entities continued accessing DMV records through the ExpressNet portal for approximately three months before Defendants discovered this activity on September 27, 2021 (*id.* ¶¶ 4, 78).

On November 4, 2021, ISO Claims sent a letter to Cantinieri, notifying her of the “data breach.” (*Id.* ¶¶ 15, 80.) The letter provided that “[i]t appears an unauthorized entity obtain[ed] credentials to access [the ExpressNet] portal as early as July 5, 2021, and to obtain . . . certain

² Excerpts from the parties’ submissions are reproduced here exactly as they appear in the original. Unless otherwise noted, errors in spelling, punctuation, or grammar will not be corrected or highlighted.

motor vehicle reports containing driver names, dates of birth, addresses, and driver's license numbers.” (*Id.* ¶ 80.)

The Amended Complaint alleges that Cantinieri has suffered numerous injuries and faces additional imminent or impending injuries due to Defendants' failure to prevent or detect the disclosure of Cantinieri's DMV records to unauthorized entities or cybercriminals. (*Id.* ¶¶ 7, 17.)

First, the Amended Complaint alleges that Cantinieri has been injured by the disclosure of her PII itself, and that such disclosure violated Cantinieri's rights to privacy and rights under the DPPA. (*Id.* ¶ 7.)

Second, the Amended Complaint alleges that Cantinieri has received an increased number of phishing email attempts and fraudulent phone calls following the disclosure of her PII. (*Id.*)

Third, the Amended Complaint alleges that Cantinieri suffered specific instances of identity theft and financial fraud and resulting consequences. (*Id.* ¶¶ 117–29.) Specifically, the Amended Complaint alleges that unauthorized entities used Cantinieri's PII to apply for unemployment assistance on April 4, 2021 (*id.* ¶ 118), to open a bank membership on August 8, 2021 (*id.* ¶ 122), and to apply for various loans on the following dates: June 4, 2021; July 2, 2021; August 8, 2021; August 9, 2021; August 17, 2021; and sometime before August 18, 2021 (*see id.* ¶¶ 119–21, 123, 127). The Amended Complaint alleges that Cantinieri suffered another incident of identity theft around one year later, on June 10, 2022, when Cantinieri “unfroze her credit for the purposes of leasing a new motor vehicle” and “a cybercriminal submitted an application for an online loan for a tablet” within twenty-four hours. (*Id.* ¶ 129.) “[T]he company

contacted [Cantinieri] before approving the loan and she was able to cancel the order before any charges on her credit were incurred.” (*Id.*)

The Amended Complaint alleges that Catinieri suffered additional injuries as a result of these instances of identity theft and financial fraud, including: “lowered credit scores resulting from credit inquiries following fraudulent activity”; “costs associated with the detection . . . of identity theft and financial fraud”; “costs associated with time and the loss of productivity spent addressing and attempting to monitor, ameliorate, mitigate, and deal with the consequences of the data breach”; and “stress, nuisance, and annoyance from dealing with the consequences of the data breach.” (*Id.* ¶ 7.) For example, the Amended Complaint alleges that Catinieri froze her credit indefinitely at the advice of credit agencies after the initial series of fraudulent applications were submitted in her name, which has “caused damages and inconvenience,” because Catinieri has not been able to “conduct ordinary consumer transactions without significant difficulty[] [and] inconvenience” (*Id.* ¶ 128.)

Fourth, the Amended Complaint alleges that Catinieri has suffered “damages to and diminution in value of” her PII and damages to “the retention of the reasonable value of the PII still in Defendants’ possession.” (*Id.* ¶ 99.)

Fifth, the Amended Complaint alleges that Catinieri faces “imminent or impending risk of future harm” due to Defendants’ actions, including an “increased risk of future identity theft and financial fraud posed by ill-intentioned unauthorized entities or criminals possessing [her] PII”; and “the continued risk to [her] PII which remains in the possession of Defendants and is

subject to further data breaches so long as Defendants fail to undertake appropriate and adequate cybersecurity measures.” (*Id.*)

Sixth, the Amended Complaint also alleges that in addition to injuries resulting from *prior* acts of identity theft, Cantinieri has incurred “costs associated with the . . . *prevention* of identity theft and financial fraud.” (*Id.* ¶ 7 (emphasis added).) Cantinieri alleges that she “cannot conduct ordinary consumer transactions” because she froze her credit card due to the “ongoing threat of future acts of identity theft.” (*Id.* ¶ 128.) The Amended Complaint also alleges “emotional anguish and distress, including, but not limited to fear and anxiety related to the exposure and exploitation of her PII and resulting vulnerability to imminent and impending identity theft or financial fraud in the future.” (*Id.* ¶ 17.)

Defendants dispute the Amended Complaint’s allegations that Cantinieri’s PII was exposed to unauthorized third parties through the ExpressNet portal on June 5, 2021, or earlier and that Cantinieri’s SSN was *ever* disclosed to an unauthorized third party through the ExpressNet portal. (Defs.’ Mem. Supp. Mot. Dismiss (“Defs.’ Mem.”) at 3–4, ECF No. 79-1.) Defendants have submitted evidence that the only record or data disclosed through the ExpressNet portal that included Cantinieri’s information was her New York State motor vehicle record, which did *not* include Cantinieri’s SSN, and that her motor vehicle record was not disclosed to an unauthorized third party until September 23, 2021. (*Id.* at 4–5.) Defendants argue that these facts defeat jurisdiction for two reasons: (1) Cantinieri’s alleged injuries predating the September 23, 2021 disclosure of her motor vehicle record to third parties cannot plausibly result from that disclosure and therefore do not support standing for her claims; and (2) Cantinieri’s alleged injuries after September 23, 2021 were not plausibly caused by the alleged data

disclosure because the specific injuries pled would have required disclosure of her SSN, which was never disclosed to any unauthorized party. (*Id.*)

II. Factual Submissions Relating to Standing

To contest the Amended Complaint's factual allegations concerning Cantinieri's standing, Defendants submitted their responses to several of Cantinieri's Interrogatories, which were all certified by Michael Snook, an iiX employee, on behalf of Defendants to be true to the best of his "knowledge, information and belief" and "prepared with the assistance and advice of counsel and the assistance of [Defendants'] employees and representatives." (*See* Defs.' Resps. to Pl.'s Interrog. Nos. 5, 17–19, Defs.' Mot. Ex. 1, ECF No. 79-2; Defs.' Supp. Resp. to Pl.'s Interrog. No. 17, Defs.' Mot. Ex. 2, ECF No. 79-3.)

In these interrogatory responses, Defendants asserted that the ExpressNet portal "is not a database" but "provides a gateway for customers to request copies of motor vehicle reports and driving histories." (Defs.' Resp. to Pl.'s Interrog. No. 5, Defs.' Mot. Ex. 1 at 4.) Defendants defined the ExpressNet portal's customers as "companies that have a permissible purpose to evaluate an individual's driving history, such as a trucking company evaluating an employment application for a new commercial driver." (*Id.*) Defendants stated that a company must submit supporting documentation in order to obtain an authorized ExpressNet portal account that can submit requests for motor vehicle reports. (*See* Defs.' Supp. Resp. to Pl.'s Interrog. No. 17, Defs.' Mot. Ex. 2 at 4.) Defendants further asserted that iiX conducts a due diligence analysis of any new customer account to ensure that the applicant has an "appropriate and legitimate business interest" before it will authorize that account. (Defs.' Resp. to Pl.'s Interrog. No. 5, Defs.' Mot. Ex. 1 at 4.) Defendants also submitted iiX's insurance subscription agreement showing the information that a purported ExpressNet customer must provide to iiX before it can

obtain a customer account, which includes, among other things, the company's name, mailing address, physical address, website, type of business, reason for ordering services, and federal tax ID. (iiX Contract, Defs.' Mot. Ex. 10, ECF No. 79-11.) The agreement also states that a company must provide documentation of a current and valid business license or a copy of a current state sales and use tax certificate or official federal tax documents from within the past year. (*Id.*)

In Defendants' response to Cantinieri's Interrogatories, Defendants also provided the following information about how iiX discovered and identified all activity made by fraudulent accounts on the ExpressNet portal. On September 27, 2021, a former product manager at iiX first discovered activity on the ExpressNet portal by a fraudulent actor using an account mimicking an insurance company named "The Insurance Mart, Inc." (Defs.' Resp. to Pl.'s Interrog. No. 18, Defs.' Mot. Ex. 1 at 6–7.) Once iiX discovered this fraudulent account, iiX investigated its records to uncover any additional fraudulent accounts created by the same actor and took the following steps to identify all of the accounts that the fraudulent actor had used to access the ExpressNet portal. (Defs.' Supp. Resp. to Pl.'s Interrog. No. 17.)

First, iiX performed an "IP address analysis" to identify all unique IP addresses used to access the "The Insurance Mart, Inc." account within the ExpressNet portal and to search all other ExpressNet records to identify other accounts accessed from the same IP addresses from September 2014 through September 2021. (*Id.* at 3.) iiX repeated this process with the additional accounts that were uncovered until no new accounts or IP addresses were identified. (*Id.*)

Second, iiX conducted a "Web Application Firewall . . . Analysis" of all available records of ExpressNet portal activity from July 2021 to September 2021 to identify any additional IP addresses used by the fraudulent actor to visit Verisk websites. (*Id.*) iiX used the IP addresses discovered in the analysis to identify the unique identifiers, or "cookies," that the Verisk Web

Application Firewall assigned to the fraudulent actor, and then used those cookies to find all IP addresses associated with those cookies. (*Id.* at 3–4.)

Third, iiX analyzed the email domains within its records to confirm that there were no additional fraudulent accounts. (*Id.* at 4.) iiX discovered that the email domains used by the fraudulent entity to access the ExpressNet portal had all been registered with the “Namecheap” registrar, had all been registered within ten days of first being used to communicate with iiX, and had all been created within ninety days of each other. (*Id.*) iiX then analyzed all ExpressNet portal accounts that had been created or modified between August 2020 and September 2021 to identify any email addresses that had been registered with the Namecheap registrar and discovered no additional fraudulent accounts. (*Id.*)

Fourth, iiX conducted an audit of all documents submitted in support of applications for new ExpressNet portal accounts from January 1, 2021 through November 8, 2021. (*Id.* at 4.) iiX reviewed the documents to ensure, among other things, that all requisite documentation was collected, that there were no inconsistencies within the applications, and that the documentation “matched with available database and state registration information.” (*Id.*) Again, iiX was able to confirm that there were no additional fraudulent accounts within the ExpressNet portal. (*Id.* at 4–5.)

After iiX identified all of the accounts that the fraudulent entity used to access the ExpressNet portal, iiX conducted an analysis of account creation and transactions histories to identify the date each fraudulent account was created and the dates on which fraudulent accounts requested information through the ExpressNet portal. (Defs.’ Resp. to Pl.’s Interrog. No. 17, Defs.’ Mot. Ex. 1 at 5.) iiX records every customer transaction within the ExpressNet portal and stores those records for ninety (90) days. (Defs.’ Resp. to Pl.’s Interrog. No. 5, Defs.’ Mot. Ex. 1

at 4.) This data is “securely stored in accordance with iiX’s obligations under its contractual agreements with individual states” and is “not accessible to any external parties.” (*Id.*)

Through this investigation, iiX determined that it “was not subject to a cyber intrusion” and that “the earliest date of unauthorized access to *any* individual motor vehicle report was July 5, 2021.” (Defs.’ Resp. to Pl.’s Interrog. No. 17, Defs.’ Mot. Ex. 1 at 6 (emphasis added).)

Defendants also submitted an excerpt of the transcript of Michael Snook’s deposition in which Snook testified that, based on his and his team’s investigation of this incident, the first date that the fraudulent actor was able to access a motor vehicle report through the ExpressNet portal was July 5, 2021. (Snook Dep. 76:4–10, Defs.’ Mot. Ex. 9, ECF No. 79-10).

Defendants asserted in their interrogatory answers that iiX was also able to determine that on September 23, 2021, the fraudulent entity used the ExpressNet portal to “request a copy of Plaintiff’s motor vehicle report from the State of New York.” (Defs.’ Resp. to Pl.’s Interrog. No. 19, Defs.’ Mot. Ex. 1 at 8.) In order to obtain this report, the fraudulent entity “inputted Plaintiff’s driver’s license number and associated state.” (*Id.*) “The motor vehicle report accessed contained Plaintiff’s name, date of birth, address, and driver’s license number.” (*Id.*) It did not include Cantinieri’s SSN. (*See id.*)

To further confirm that Cantinieri’s data was not accessed until September 23, 2021, and to show the extent of the PII that was disclosed, Defendants submitted Cantinieri’s motor vehicle report dated September 23, 2021, and a webpage about driving records published by the New York Department of Motor Vehicles (“New York DMV”). (Cantinieri’s MVR, Defs.’ Mot. Ex. 5, ECF No. 79-6; NY DMV Driving Records Info., Defs.’ Mot. Ex. 6, ECF No. 79-7).

Cantinieri’s September 23, 2021 motor vehicle report states that it was prepared for “The Insurance Mart Inc.” and provided through iiX and includes Cantinieri’s first and last name,

address, driver's license number, date of birth, driver description (including gender, height, and eye color), "client ID#," "MI #," the driver's license class, status, expiration, and restrictions, and activity related to license points reductions. (Cantinieri's MVR.) The New York DMV webpage explains that "[t]he DMV collects your Social Security Number (SSN) when you apply for a NYS driver license. Your SSN *does not appear* on records or documents issued by the DMV." (NY DMV Driving Records Info. at 2 n.2 (emphasis added).)

In support of the Motion to Dismiss, Defendants also submitted a November 4, 2021 letter from Defendants to Cantinieri notifying her of the "security incident." (Disclosure Ltr., Defs.' Mot. Ex. 4, ECF No. 79-5.) This letter states, among other things, that Defendants had "deactivated accounts identified with suspicious activity" following their investigation into the incident, and that they had "engaged leading investigations experts to assist with an investigation to determine the nature and scope of the incident." (*Id.* at 2.)

Defendants also submitted the Executive Summary prepared by CrowdStrike Services, an independent cybersecurity company, which conducted a forensic analysis of the ExpressNet web portal security incident, and the declaration of Matthew Harvey, the director of professional services at CrowdStrike. (CrowdStrike Exec. Summ., Defs.' Mot. Ex. 8, ECF No. 79-9.) The Executive Summary summarizes key findings from CrowdStrike's analysis of iiX's data, and states that the "earliest evidence of unauthorized activity that CrowdStrike identified occurred on May 25, 2021" when an unauthorized entity submitted an application for a customer account, imitating The Insurance Mart, Inc. (*Id.* at 4.) CrowdStrike also found that an unauthorized entity successfully obtained seven different customer accounts, imitating different legitimate insurance

companies, and then used six of those accounts to make unauthorized requests for data from various DMVs through the ExpressNet portal. (*Id.*)

Finally, Defendants submitted excerpts from the transcripts of two pre-trial conferences in this case. The first is from the transcript of a May 9, 2023 conference before Judge Joan M. Azrack, to whom this case was previously assigned, in which Judge Azrack stated that “whether social security numbers were exposed” in the security incident was “entirely dispositive” of Cantinieri’s standing to pursue this action. (May 9, 2023 Conf. Tr., Defs.’ Mot. Ex. 1, ECF No. 79-2.) The second is from the transcript of a July 19, 2023 conference before Magistrate Judge James M. Wicks, to whom jurisdictional discovery was referred, regarding the need for additional jurisdictional discovery. (Tr. of July 19, 2023 Conf., Defs.’ Mot. Ex. 3, ECF No. 79-4; *see also* ECF Nos. 51, 59.) At this latter conference, Cantinieri’s counsel represented that the security incident involving the disclosure of Cantinieri’s PII “wasn’t a cyber intrusion. This was an act of negligent credentialing by the defendant. Nobody broke in, nobody hacked in.” (Tr. of Jul. 19, 2023 Conf. at 22:9–12.) Cantinieri’s counsel also stated that “defendants have proven . . . that an MVR from New York State DMV doesn’t have a field for a social security number,” which is something that “Plaintiffs do not dispute.” (*Id.* at 23:14–19.)

In opposition to the Motion to Dismiss, Cantinieri filed duplicates of certain defense exhibits.³ Cantinieri also filed a longer excerpt of the Snook Deposition transcript than what Defendants submitted. (Snook Dep. 30–41, Pl.’s Opp’n Ex. 3, ECF No. 79-15.) In the excerpt, Cantinieri’s counsel asked Snook whether iiX “investigat[ed] whether or not an individual

³ See Pl.’s Opp’n Ex. 1, ECF No. 79-13 (duplicate of Defs.’ Mot. Ex. 8 at 4–5); Pl.’s Opp’n Ex. 2, ECF No. 79-14 (duplicate of Defs.’ Mot. Ex. 4); Pl.’s Opp’n Ex. 4, ECF No. 79-16 (duplicate of Defs.’ Mot. Ex. 5); Pl.’s Opp’n Ex. 5, ECF No. 79-17 (duplicate of Defs.’ Mot. Ex. 2).

accessing the [ExpressNet] portal through credentials provided by defendants, would be able to obtain Social Security numbers or other [PII]” (*Id.* at 30:8–15.) Snook testified:

[W]e know what data exactly comes back from New York We know what New York says it includes in document responses, we also know what it says it does not include, which is Social Security number, and we know that our portal, what it does is, it takes input as a driver’s license number and goes and makes a request with just that driver’s license number and all that returns. From that point on, there’s no control from the user. And at that point on, it returns just the motor vehicle record data. Which, again, only contains the PII elements that I stated earlier. So that we understand and we know. It’s how we designed our application. It is, again, to the best of my knowledge, exactly how the application works. I’m not sure—I’m not understanding what there is to investigate there. It’s how the application works I can’t speculate as to what else we would do beyond reviewing and understanding how our application works and what data comes back. . . . With the steps that I outlined, we were highly confident that we understood the full extent of the data and scope for this issue.

(*Id.* at 35:15–16, 35:20–25, 36:1–15; 36:17–20; 38:1–4.)

Cantinieri also submitted Defendants’ response to Plaintiffs’ Interrogatory Number 23, which asked how Defendants had identified or determined that the scope of the Cantinieri’s PII exposed to a fraudulent entity only included “driver names, dates of birth, addresses, and driver’s license numbers,” as Defendants had stated in their November 5, 2021 notification letter. (Defs.’ Resp. to Pl.’s Interrog. No. 23, Pl.’s Opp’n Ex. 6, ECF No. 79-18.) Defendants responded that they had identified that only these elements of Cantinieri’s data may have been exposed because only these PII elements are included in New York motor vehicle reports. (*Id.* at 3.)

On reply, Defendants submitted another excerpt from the transcript of the July 19, 2023 conference before Judge Wicks. (Jul. 19, 2023 Conf. Tr. at 37–38, 43, Defs.’ Reply Ex. 1, ECF No. 79-20.) In that conference, Judge Wicks stated to Plaintiffs’ counsel: “[Y]ou didn’t proffer

anything, an expert affidavit, declaration, anything saying that there's a possibility that [an SSN] could be accessed" through the ExpressNet portal. (*Id.* at 38:14–16.)

PROCEDURAL HISTORY

I. The Original Complaint and Defendants' First Motion to Dismiss

On December 15, 2021, Cantinieri filed the class action complaint in this action alleging that Defendants' failure to safeguard her PII from an unauthorized actor through their web portal resulted in Cantinieri's loss of privacy and numerous incidents of identity theft and financial fraud against her. (Compl. ¶¶ 1, 12, ECF No. 1.) Defendants moved to dismiss the complaint under Rule 12(b)(1) and (b)(6). (Mot. Dismiss Compl., ECF No. 26; *see also* ECF Nos. 35, 39, 44.) Defendants argued, among other things, that Cantinieri does not have standing because her alleged injuries could not plausibly have been caused by Defendants' disclosure of her PII to an unauthorized entity. (Mot. Dismiss Compl. at 1.) Defendants challenged the complaint's factual allegations as to the timing and scope of the disclosure of Cantinieri's PII to a third-party posing as a customer, asserting that some alleged injuries pre-dated the disclosure of her PII and others required information that was never disclosed by Defendants, namely her SSN. (*See id.* at 1–10.)

On March 31, 2023, Judge Azrack directed the parties to conduct focused jurisdictional discovery concerning the timing and scope of the disclosure of Cantinieri's PII to determine whether Cantinieri has Article III standing to bring the claims pled in the complaint. (Order Denying Mot. Dismiss, ECF No. 49.) Judge Azrack denied Defendants' motion to dismiss the complaint with leave to renew after the completion of jurisdictional discovery. (*Id.*)

II. Jurisdictional Discovery

On May 9, 2023, Judge Azrack referred the parties to Judge Wicks for jurisdictional discovery on two issues: (1) whether Cantinieri's SSN was disclosed by Defendants to the

unauthorized entities, and (2) when the disclosure of Cantinieri's PII occurred. (Min. Entry, May 9, 2023; ECF No. 51.)

On October 10, 2023, this case was reassigned to my docket. (Elec. Not., Oct. 10, 2023.) In a status conference before me on November 20, 2023, the parties confirmed that jurisdictional discovery was complete. (Min. Entry, Nov. 20, 2023.) I granted Cantinieri leave to file an amended complaint and issued a briefing schedule for Defendants' anticipated motion to dismiss the forthcoming amended complaint under Rule 12(b)(1) and 12(b)(6). (*Id.*)

III. Amended Complaint and Defendants' Second Motion to Dismiss

On December 15, 2023, Cantinieri timely filed the Amended Complaint, which is the operative complaint in this action. (Am. Compl., ECF No. 72.) The Amended Complaint asserts seven claims: (1) negligence (*id.* ¶¶ 163–75); (2) negligence per se under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 (*id.* ¶¶ 177–82) and negligence per se under the Driver's Privacy Protection Act, 18 U.S.C. § 2721–2725 ("DPPA") (*id.* ¶¶ 183–93); (3) violations of the DPPA, 18 U.S.C. §§ 2721–2725 (*id.* ¶¶ 194–208); (4) unjust enrichment (*id.* ¶¶ 209–21); (5) a Declaratory Judgment Act claim, 28 U.S.C. § 2201, *et seq.* (*id.* ¶¶ 222–33); (6) violation of the New York General Business Law ("GBL") § 899-aa (*id.* ¶¶ 234–42); and (7) violation of GBL § 349 (*id.* ¶¶ 243–54). Cantinieri seeks to bring the first five claims on behalf of herself, a proposed nationwide class, and a proposed New York class. (*Id.* ¶ 151.) She seeks to bring the sixth and seventh claims under the New York GBL on behalf of herself and a proposed New York class, but not the proposed nationwide class. (*Id.* ¶ 152.) The seven claims alleged in

the Amended Complaint mirror the claims asserted in the initial complaint with the exception of the additional DPPA claims. (*Compare* Compl. at 22–36 with Am. Compl. at 34–53.)

The Amended Complaint seeks “preliminary and equitable relief”⁴ and monetary damages for the DPPA claim. (Am. Compl. at 44.) It also seeks declaratory relief, injunctive relief, and damages for the Declaratory Judgment Act claim and the New York GBL §§ 899-aa and 349 claims. (*Id.* at 48, 50–51, 53.) The Amended Complaint also seeks monetary damages for the claims of negligence, negligence per se under the FTC Act and the DPPA, and unjust enrichment. (*Id.* at 37–39, 46.)

On February 29, 2024, Defendants filed their fully briefed Motion to Dismiss the Amended Complaint pursuant to Rule 12(b)(1) and (b)(6) (the “Motion”). (ECF No. 79.) In support of their Motion, Defendants submitted a memorandum and evidence. (Defs.’ Mem., ECF No. 79-1; ECF No. 79-2–11.) Cantinieri submitted an opposition brief and supporting evidence. (Pl.’s Opp’n, ECF No. 79-12; ECF Nos. 79-13–18.) Defendants submitted a reply and a supporting exhibit. (Defs.’ Reply, ECF No. 79-19; ECF No. 79-20.)

JURISDICTION

The Amended Complaint asserts that this Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because one of Cantinieri claims arises under a federal statute, 18 U.S.C. § 2721, *et seq.* (Am. Compl. ¶ 63.) It also asserts that the Court has supplemental jurisdiction over Cantinieri’s state law claims under 28 U.S.C. § 1367(a) because these claims are part of the same case or controversy as the federal claim. (*Id.* ¶ 65.)

⁴ Cantinieri has not filed a motion for a preliminary injunction in this action.

Nevertheless, as discussed below, this Court lacks subject matter jurisdiction under Article III because Cantinieri does not have standing to pursue the claims pled in the Amended Complaint.⁵

LEGAL STANDARDS

I. Lack of Subject Matter Jurisdiction under Rule 12(b)(1)

A district court properly dismisses a case under Rule 12(b)(1), Fed. R. Civ. P., when the court “lacks the statutory or constitutional power to adjudicate it, such as when . . . the plaintiff lacks constitutional standing to bring the action.” *Cortlandt St. Recovery Corp. v. Hellas Telecomms., S.a.r.l.*, 790 F.3d 411, 416–17 (2d Cir. 2015).⁶ The Second Circuit has recognized that, at the pleading stage, “a Rule 12(b)(1) motion challenging subject matter jurisdiction may be either facial, i.e., based solely on the allegations of the complaint and exhibits attached to it, or fact-based, i.e., based on evidence beyond the pleadings.” *Harty*, 28 F.4th at 441. When a party raises a facial challenge to the court’s subject matter jurisdiction, “the plaintiff has no evidentiary burden”; the district court need only “determine whether the [p]leading alleges facts that affirmatively and plausibly suggest that the plaintiff has standing to sue.” *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 56 (2d Cir. 2016); *see also Lugo*, 114 F.4th at 87. In assessing a facial challenge to standing, a court “must take all uncontroverted facts in the

⁵ Defendants do not raise personal jurisdiction or insufficient service of process defenses under Rule 12(b)(2) and (b)(5), and such defenses are therefore waived. *See* Fed. R. Civ. P. 12(b) (“A motion asserting [a Rule 12(b)(2) or (b)(5) defense] must be made before pleading if a responsive pleading is allowed.”); Fed. R. Civ. P. 12(h)(1)(B) (“A party waives any defense listed in Rule 12(b)(2)–(5) by . . . failing to . . . make it by motion under this rule.”). Moreover, venue in the Eastern District of New York is proper under 28 U.S.C. § 1391(b)(2) because “a substantial part of the events giving rise to this action occurred in this District” and because “Defendants transact substantial business generally in this District.” (Am. Compl. ¶ 67.)

⁶ Unless otherwise indicated, all internal citations, quotation marks, and alterations are omitted.

complaint (or petition) as true, and draw all reasonable inferences in favor of the party asserting jurisdiction.” *Tandon*, 752 F.3d at 243.

When a party has placed jurisdictional facts into dispute by “offer[ing] extrinsic evidence that contradicts the material allegations of the complaint,” however, “the court has the obligation to decide issues of fact by reference to evidence outside the pleadings, such as affidavits.” *Harty*, 28 F.4th at 442. When the extrinsic evidence “reveals the existence of factual problems,” the plaintiff “will need to come forward with evidence controverting that presented by the defendant regarding standing.” *Lugo*, 114 F.4th at 87. “In that case, the party asserting subject matter jurisdiction has the burden of proving by a preponderance of the evidence that it exists.” *Tandon*, 752 F.3d at 243; *Katz v. Donna Karan Co., L.L.C.*, 872 F.3d 114, 120 (2d Cir. 2017) (same). “[I]f the evidence proffered by the defendant is immaterial because it does not contradict plausible allegations that are themselves sufficient to show standing,” the plaintiffs “are entitled to rely” on the complaint’s allegations. *Carter*, 822 F.3d at 57–58.

“If the court determines at any time that it lacks subject-matter jurisdiction, the court must dismiss the action.” Fed. R. Civ. P. 12(h)(3). A court considers a Rule 12(b)(1) challenge before other arguments for dismissal because dismissal for lack of subject matter jurisdiction renders a defendant’s defenses and objections moot. *Daly v. Citigroup Inc.*, 939 F.3d 415, 426 (2d Cir. 2019); *see also Pressley v. City of New York*, No. 11-cv-3234, 2013 WL 145747, at *5 (E.D.N.Y. Jan. 14, 2013) (“A court faced with a motion to dismiss pursuant to both Rule 12(b)(1) and (b)(6) must decide the jurisdictional question first because a disposition of a Rule 12(b)(6) motion is a decision on the merits and, therefore, an exercise of jurisdiction.”).

II. Article III Standing

Article III of the Constitution “limits the federal judicial power to deciding ‘Cases’ and ‘Controversies.’” *Soule v. Conn. Ass’n of Sch.*, 90 F.4th 34, 45 (2d Cir. 2023) (citing U.S. Const. art. III § 2). A case or controversy only exists when the plaintiff has “standing” to sue because they have “a personal stake in the outcome of the litigation.” *Id.* (citing *United States v. Texas*, 599 U.S. 670 (2023)). “In a class action, federal courts lack jurisdiction if no named plaintiff has standing.” *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 299 (2d Cir. 2021).

In order to establish Article III standing, a plaintiff must show: “(1) that they suffered an injury in fact, (2) that the injury is fairly traceable to Defendants’ challenged conduct, and (3) that the injury is likely to be redressed by a favorable judicial decision.” *Soule*, 90 F.4th at 45 (citing *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016)). A “plaintiff must demonstrate standing for each claim that they press and for each form of relief that they seek.” *Id.* (citing *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021)).

A. Injury in Fact

In order to demonstrate an “injury in fact,” a plaintiff must establish “an invasion of a legally protected interest which is (a) concrete and particularized . . . and (b) actual or imminent, not conjectural or hypothetical.” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992); *see also Soule*, 90 F.4th at 45, 50 (citing *TransUnion*, 594 U.S. at 423).

a. Concrete

An injury is “concrete” when it is “real, and not abstract.” *Soule*, 90 F.4th at 45. A concrete injury is one that has “a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts”—such as physical harm, monetary harm, or

various intangible harms. *TransUnion*, 594 U.S. at 417 (quoting *Spokeo*, 578 U.S. at 340–41); *Salazar v. Nat’l Basketball Ass’n*, 118 F.4th 533, 541–42 (2d Cir. 2024).

b. Particularized

An injury is “particularized” only when it “affect[s] the plaintiff in a personal and individual way.” *Soule*, 90 F.4th at 45–46 (citing *Spokeo*, 578 U.S. at 339).

c. Actual or Imminent

Even where an injury is concrete and particularized, it must also be “actual or imminent” to constitute an Article III injury in fact. *Soule*, 90 F.4th at 45, 50 (citing *TransUnion*, 594 U.S. at 423). An injury is “imminent” when “threatened injury is certainly impending, or there is a substantial risk that the harm will occur.” *Bohnak v. Marsh & McLennan Cos.*, 79 F.4th 276, 288 (2d Cir. 2023); *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014).

For a declaratory or injunctive relief claim, a plaintiff “cannot rely on past injury to satisfy the injury requirement but must show a likelihood that they will be injured in the future.” *Dorce v. City of New York*, 2 F.4th 82, 95 (2d Cir. 2021). To do so, a plaintiff must establish that “the threatened injury is certainly impending, or [that] there is a substantial risk that the harm will occur.” *Id.* (citing *Susan B. Anthony List*, 573 U.S. at 158).

Where a plaintiff’s PII “has been compromised but not yet misused,” the Second Circuit has instructed courts to consider “three non-exhaustive factors” to determine whether the plaintiff faces “a substantial risk of harm” that can support Article III standing. *Bohnak*, 79 F.4th at 288. These so-called *McMorris* factors are the following:

- (1) whether the plaintiffs’ data has been exposed as the result of a targeted attempt to obtain that data;
- (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and

(3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

McMorris, 95 F.3d at 303; *see also Bohnak*, 79 F.4th at 288.

The Second Circuit has established that “where plaintiffs have shown a substantial risk of future identity theft or fraud, “any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact.” *McMorris*, 995 F.3d at 303. Where plaintiffs “have not alleged a substantial risk of future identity theft,” however, “the time they spent protecting themselves against this speculative threat cannot create an injury.” *Id.*; *see also Bohnak*, 79 F.4th at 286–87 (finding that the plaintiff alleged concrete harms due to a “material risk of future harm” arising from the “exposure of [her] PII to a malign outside actor,” including “incurred out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft[,] . . . lost time[,] and other opportunity costs associated with attempting to mitigate the consequences of the data breach”).

A plaintiff can allege an *actual* injury to support standing for declaratory and injunctive relief by alleging facts that demonstrate that the plaintiff’s PII has been disclosed *and* is being misused by the recipient. *See Salazar*, 118 F.4th at 544 (finding that the alleged injury in fact was actual where the defendant disclosed plaintiff’s PII to a company that uses the information “to show the [plaintiff] targeted ads . . . for its own commercial purposes, not the [defendant’s] or the [plaintiff’s] purposes”).

B. Traceability

“The traceability requirement for Article III standing means that the plaintiff must demonstrate a causal nexus between the defendant’s conduct and the injury.” *Chevron Corp. v. Donziger*, 833 F.3d 74, 121 (2d Cir. 2016). A plaintiff’s injury must also be “fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third

party not before the court.” *Ateres Bais Yaakov Acad. of Rockland v. Town of Clarkstown*, 88 F.4th 344, 352–53 (2d Cir. 2023) (citing *Carter*, 822 F.3d at 55–56). An injury, however, “need not be directly attributable to a defendant.” *Carter*, 822 F.3d at 59. The Second Circuit has impressed that this is not “an onerous standard” but is “a standard lower than that of proximate causation.” *Id.* at 55.

C. Redressability

In order for a plaintiff to establish that their injury in fact is redressable, “a plaintiff must show that it is likely, as opposed to merely speculative, that the alleged injury will be redressed by a favorable decision.” *Soule*, 90 F.4th at 47 (citing *Lujan*, 504 U.S. at 561). “A plaintiff makes this showing when the relief sought would serve to eliminate any effects of the alleged legal violation that produced the injury in fact.” *Id.* (citing *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 105–06 (1998)).

DISCUSSION

Cantinieri lacks Article III standing to bring any of the seven claims in the Amended Complaint. The Amended Complaint seeks damages for each claim as well as “preliminary and equitable relief” for the DPPA claim and declaratory and injunctive relief for claims under the Declaratory Judgment Act and New York GBL §§ 899-aa and 349. (Am. Compl. at 38, 43, 48, 50–51, 53.) Cantinieri has failed to establish Article III standing with respect to any of these claims because she has not shown that her alleged injuries are actual or imminent such that they constitute injuries in fact or that they are fairly traceable to Defendants’ disclosure of her PII through the ExpressNet portal. I address each of Cantinieri’s alleged injuries in turn.

I. The Disclosure of Cantinieri's PII

The Amended Complaint alleges that the disclosure of Cantinieri's PII to a fraudulent actor was itself an injury in fact. (Am. Compl. ¶ 7.) Cantinieri argues that this disclosure alone confers standing because it constituted a violation of the DPPA and her right to privacy. (Pl.'s Opp'n at 7; *see also* Am. Compl. ¶ 19.) Cantinieri is incorrect. While the disclosure of Cantinieri's PII satisfies the requirement for an injury in fact that is concrete and particularized, Cantinieri has not shown that this injury is actual or imminent as required to support Article III standing for claims for damages and declaratory and injunctive relief.

As an initial matter, the Supreme Court has clarified that where “a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right,” a defendant's violation of that statute does not “automatically satisf[y] the injury-in-fact requirement.” *TransUnion*, 594 U.S. at 426. Thus, contrary to Cantinieri's contention, the alleged violation of the DPPA does not automatically constitute an injury in fact for Article III standing. *Id.*

Where, like here, a plaintiff has alleged that a defendant disclosed their “personally identifiable information . . . to an unauthorized third party,” the disclosure itself is “sufficiently concrete” to constitute an injury in fact because such an injury is “closely related” to the public disclosure of private facts—an intangible harm traditionally recognized at common law. *Salazar*, 118 F.4th at 541–42; *see also Bohnak*, 79 F.4th at 285–86 (same). Thus, the disclosure of Cantinieri's PII satisfies the “concreteness” requirement for an injury in fact to support

Cantinieri's damages claims. Additionally, because the disclosure concerns Cantinieri's PII, it also satisfies the requirement that the alleged injury be "particularized." *Soule*, 90 F.4th at 45–46.

Cantinieri still must demonstrate, however, that the concrete and particularized injury of the disclosure of her PII to a fraudulent actor is actual or imminent in order to demonstrate Article III standing to bring her claims. *See Bohnak*, 79 F.4th at 287 ("[T]he conclusion that [an] injury is concrete does not fully resolve the standing question because it addresses only one component of injury in fact."). The Second Circuit has clarified that to establish an injury in fact based on the disclosure of a plaintiff's PII, the plaintiff must either demonstrate actual injuries resulting from the disclosure or "a substantial risk of harm" under the *McMorris* factors. *Bohnak*, 79 F.4th at 288 (citing *McMorris*, 95 F.3d at 303); *see also McMorris*, 95 F.3d at 303 (finding no standing where the plaintiffs alleged that their PII had been disclosed but did not allege that the disclosed information had been used or that they faced a substantial risk of harm based on the disclosure).

Cantinieri argues that the very fact that her PII was disclosed to a fraudulent actor on the ExpressNet platform satisfies the "actual or imminent" injury requirement for establishing an injury in fact. *Soule*, 90 F.4th at 45, 50 (citing *TransUnion*, 594 U.S. at 423); Pl.'s Opp'n at 7. This argument is squarely contradicted by the Second Circuit's holding in *Bohnak* that a plaintiff had established an injury in fact based on disclosure of her PII only where she *also* established a substantial risk of harm from the disclosure under the *McMorris* factors. *Bohnak*, 79 F.4th at 288. In other words, the mere disclosure of the plaintiff's PII to an unauthorized actor did not, standing alone, establish the injury in fact required for Article III standing to bring claims targeting the defendants' disclosure of Bohnak's PII. *See id.* This principle is also supported by the Second Circuit's decision in *Salazar*, where the plaintiff was found to have shown an injury

in fact where the National Basketball Association (“NBA”) disclosed to Meta the plaintiff’s PII, which Meta allegedly “harnesses . . . to show the user targeted ads—ads that Meta chooses for its own commercial purposes, not the purposes of the NBA or the user.” 118 F.4th at 542–44.

Cantinieri relies on authority that either does not support her position or that contradicts Second Circuit authority. (Pl.’s Opp’n at 7.) For example, Cantinieri cites *Rudolph v. Hudson’s Bay Company*, a decision that cuts *against* her argument because the district court found that disclosure of the plaintiff’s PII did *not*, by itself, confer standing where the complaint did not plausibly allege a substantial risk of harm arising out of a data breach. No. 18-cv-8472, 2019 WL 2023713, at *5–6 (S.D.N.Y. May 7, 2019). Cantinieri also relies on *Rand v. Travelers Indemnity Company*, where the district court found that a plaintiff “plausibly allege[d] injury-in-fact in the form of a loss of privacy protected under the DPPA” because the “loss of privacy b[ore] a sufficiently close relationship to the tort of public disclosure of private information.” No. 21-cv-10744, 2022 WL 15523722, at *66 (S.D.N.Y. Oct. 27, 2022). (See Pl.’s Opp’n at 7.) The reasoning and conclusion of *Rand* conflicts with the Second Circuit’s holding in *Bohnak*, 79 F.4th 276, and *McMorris*, 995 F.3d 295, and I therefore decline to follow it.⁷

Thus, under Second Circuit precedents, the very fact that Cantinieri’s PII was disclosed to a fraudulent actor via the ExpressNet portal does not, by itself, establish her standing to bring

⁷ Cantinieri also relies on *Allen v. Vertafore, Inc.*, in which the district court found that an alleged violation of the DPPA was sufficient to establish an injury for Article III standing. No. 20-cv-4139, 2021 WL 3148870 (S.D. Tex. June 14, 2021), *report and recommendation adopted*, 2021 WL 3144469 (S.D. Tex. July 23, 2021), *aff’d*, 28 F.4th 613 (5th Cir. 2022). *Allen* was decided before *TransUnion*, in which the Supreme Court clarified that a statutory violation alone does not automatically confer standing. *TransUnion*, 594 U.S. at 426. Moreover, to the extent that *Allen* was not abrogated by *TransUnion*, I decline to follow it because it does not comport with the governing case law in this Circuit as set forth in *Bohnak*, 79 F.4th 276, and *McMorris*, 995 F.3d 295.

claims for damages and declaratory and injunctive relief against Defendants. *See Bohnak*, 79 F.4th at 288; *McMorris*, 95 F.3d at 303. I now turn to Cantinieri's arguments that she suffered from harms as a result of the disclosure, which support her standing to pursue the claims pled in the Amended Complaint.

II. Spam Calls and Phishing Email Messages

The Amended Complaint alleges that due to Defendants' disclosure of her PII, Cantinieri has "suffered repeated scam robocalls to her personal telephone number" and "has received numerous phishing email messages in further invasion of her personal privacy." (Am. Compl. ¶ 130.) These allegations fail to establish Cantinieri's standing to pursue claims for damages or declaratory and injunctive relief for two reasons.

First, "courts have generally rejected the theory that unsolicited calls or emails constitute an injury in fact." *Cooper v. Bonobos, Inc.*, No. 21-cv-854, 2022 WL 170622, at *5 (S.D.N.Y. Jan. 19, 2022); *Liau v. Weee! Inc.*, No. 23-cv-1177, 2024 WL 729259, at *7 (S.D.N.Y. Feb. 22, 2024) (collecting cases).

Second, even if these allegations could establish an injury in fact, the alleged injuries are not fairly traceable to the disclosure of Cantinieri's PII to a fraudulent actor through the ExpressNet portal. As an initial matter, Cantinieri has not established that Defendants *ever* disclosed her phone number or email addresses. Rather, the record shows that the PII disclosed through the ExpressNet portal did not include any email addresses or phone number for Cantinieri; it only included her New York motor vehicle record, which does not contain either piece of information. (*See* Defs.' Resp. to Pl.'s Interrog. No. 19, Defs.' Mot. Ex. 1 at 8; Cantinieri's MVR; NY DMV Driving Records Info.) Cantinieri's allegation that the disclosure of her PII resulted in an increased number of phishing emails and phone calls is implausible

because no phone number or email address was ever provided to the fraudulent actor through the ExpressNet portal. Any suggestion that an unauthorized entity could have obtained this information from the PII that was disclosed through the portal is speculative at best.

Moreover, even if Defendants had disclosed an email and/or phone number for Cantinieri, the mere allegation that she received spam calls and/or emails after the disclosure of her PII is not sufficient to establish a causal relationship between the two. *See Cooper*, 2022 WL 170622, at *5 (finding that the plaintiff’s “mere allegation” that he received spam after a security incident was not enough to show those communications were “fairly traceable” to the incident even where phone numbers and email addresses were implicated); *see also Liao*, 2024 WL 729259, at *7 (same).

Thus, Cantinieri has failed to establish that any alleged increase in her receipt of spam phone calls or emails constitute an injury in fact or that any such injury is fairly traceable to Defendants’ disclosure of her PII to the fraudulent actor through the ExpressNet portal on or around September 23, 2021.⁸

III. Past-Instances of Financial Theft and Fraud

The Amended Complaint alleges that Cantinieri experienced identity theft and financial fraud as well as consequences stemming from these incidents. (Am. Compl. ¶¶ 117–29.) These alleged injuries do not support Cantinieri’s Article III standing to pursue claims for damages, declaratory relief, or injunctive relief, however, because Cantinieri has failed to establish that any

⁸ Indeed, Cantinieri failed to address this point at all in her opposition brief (*see* Pl.’s Opp’n), even though Defendants argued in their brief that Cantinieri cannot demonstrate standing based on these emails and calls (Defs.’ Mem. at 9 n.6, 10).

of these alleged injuries are fairly traceable to Defendants' disclosure of her PII to the fraudulent actor through the ExpressNet portal.

First, Cantinieri fails to establish that fraudulent loans allegedly taken out in her name *before August 2021* are fairly traceable to the disclosure of her PII through the ExpressNet portal. Defendants have established that Cantinieri's PII was not disclosed to a fraudulent actor through the ExpressNet portal until September 23, 2021, and Cantinieri has not submitted any evidence demonstrating otherwise. (*See* Defs.' Supp. Resp. to Pl.'s Interrog. No. 17; Defs.' Resp. to Pl.'s Interrog. No. 19.) While the Amended Complaint alleges numerous instances in which Cantinieri's PII was misused by a fraudulent actor to file fraudulent applications for loans and monetary assistance in Cantinieri's name, all but one of these incidents occurred between April 2021 and August 2021—well before Cantinieri's PII was disclosed through the ExpressNet portal on September 23, 2021. (*See* Am. Compl. ¶¶ 117–29.) Because these incidents pre-date the disclosure of Cantinieri's PII, none of these fraudulent applications meet the traceability requirement of Article III standing.

Second, the Amended Complaint alleges that one fraudulent loan application was submitted in Cantinieri's name on or around June 10, 2022—more than eight months after Cantinieri's PII was disclosed. (*Id.* ¶ 129.) The Amended Complaint alleges that “a cybercriminal submitted an application for an online loan for a tablet,” but that “the company contacted Plaintiff before approving the loan and she was able to cancel the order before any charges on her credit were incurred.” (*Id.*) Defendants argue that such a loan application would have required the submission of an SSN, and that this fraudulent loan application therefore

cannot be traced to the disclosure of Cantinieri's PII to a fraudulent actor through the ExpressNet portal. (Defs.' Mem. at 8 n.4.)

As discussed, Defendants have established that Cantinieri's SSN was not disclosed through the ExpressNet portal to a fraudulent actor because that disclosure only included her New York motor vehicle record, which does not contain her SSN. (Defs.' Resp. to Pl.'s Interrog. No. 19, Defs.' Mot. Ex. 1 at 8; Cantinieri's MVR; NY DMV Driving Records Info.) Cantinieri has submitted no evidence showing otherwise.⁹ Nor does Cantinieri put forward any evidence—or even point to any allegations of the Amended Complaint—to establish that a third party could use the information that was disclosed through the ExpressNet portal to submit an application for a loan to purchase a tablet.¹⁰ For example, Cantinieri has not provided the loan application that

⁹ During the Snook Deposition, Cantinieri's counsel attempted repeatedly to elicit a response from Snook as to whether iiX investigated whether any unauthorized actor posing as an authorized customer might have been able to obtain a person's SSN located in a DMV record through the ExpressNet portal. (*See* Snook Dep. 30–41.) This line of questioning is speculative, and neither counsel's questions nor Snook's responses permit an inference that Cantinieri's SSN was disclosed, let alone prove that fact by a preponderance of the evidence.

¹⁰ Defendants have requested that I take judicial notice of the fact that “successful applications for . . . loans required the use of either a[n] SSN or an Individual Taxpayer Identification Number.” (Defs.' Mem. at 3 n.2). Defendants cite to Federal Rule of Evidence 201 (Defs.' Mem. at 3 n.2), which permits a court to take judicial notice of facts from publicly available documents that “can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.” Fed. R. Evid. 201(b)(2). Defendants have not, however, submitted a single document in the record or even cited to any publicly available document showing that a successful loan application requires the submission of either an SSN or an Individual Taxpayer Identification Number. For example, as noted above, absent from the record is even a sample application form for any of the alleged fraudulent loan applications identified in the Amended Complaint. Without knowing which documents I should consider, I cannot take judicial notice of the fact proposed by Defendants.

was submitted in her name or even a sample loan application form from the same company that would show the types of identification information required to apply for such a loan.

The Amended Complaint also alleges that Cantinieri has suffered additional injuries stemming from these alleged fraudulent loan applications, including “lowered credit scores resulting from credit inquiries following fraudulent activity”; “costs associated with the detection . . . of identity theft and financial fraud”; “costs associated with time and the loss of productivity spent addressing and attempting to monitor, ameliorate, mitigate, and deal with the consequences of the data breach”; and “stress, nuisance, and annoyance from dealing with the consequences of the data breach.” (Am. Compl. ¶ 7.) Because Cantinieri cannot establish that any of the alleged fraudulent loan applications are fairly traceable to Defendants’ disclosure of her PII, she likewise cannot meet the traceability requirement for these downstream injuries.

Cantinieri argues that these downstream injuries *are* fairly traceable to the disclosure of her PII, relying on *Cohen v. Northeast Radiology, P.C.*, No. 20-cv-1202, 2021 WL 293123, at *2 (S.D.N.Y. Jan. 28, 2021). (Pl.’s Opp’n at 10.) In *Cohen*, the district court rejected a *facial* Rule 12(b)(1) challenge, finding that the plaintiff had establish standing because allegations of a “fraudulent loan application made using his name, address, and SSN” and harms that flowed from that fraudulent loan application, such as a drop in his credit score, were fairly traceable to the alleged breach of plaintiff’s data. *Cohen*, 2021 WL 293123, at *5. *Cohen* is distinguishable from this action for two reasons. First, the plaintiff in *Cohen* alleged that the fraudulent loan application and its downstream harms occurred *after* the plaintiff’s PII was disclosed by the defendants. *Id.* Second, and most importantly, the court in *Cohen* was deciding a *facial* challenge pursuant to Rule 12(b)(1), and thus “the plaintiff [had] no evidentiary burden” and the district court only had to “determine whether the [p]leading alleges facts that affirmatively and plausibly

suggest that the plaintiff has standing to sue.” *Carter*, 822 F.3d at 56; *see also Lugo*, 114 F.4th at 87. By contrast, here, Defendants have brought a *factual* challenge to this Court’s jurisdiction over this action, and Cantinieri “has the burden of proving by a preponderance of the evidence” that subject matter jurisdiction exists. *Tandon*, 752 F.3d at 243. Because Cantinieri has failed to establish by a preponderance of evidence that any of the alleged fraudulent loan applications are fairly traceable to Defendants’ disclosure of her PII to an unauthorized actor through the ExpressNet portal on or around September 23, 2021, Cantinieri has failed to establish Article III standing with respect to any of these incidents of fraud or their attendant consequences.

IV. Diminution in the Value of Plaintiff’s PII

The Amended Complaint alleges that Cantinieri has suffered injuries in the form of “damages to and diminution in value of [her] PII” and “the retention of the reasonable value of the PII still in Defendants’ possession.” (Am Compl. ¶ 99.) Courts have found that plaintiffs fail to plausibly allege an Article III injury in fact for the diminution of the value of a plaintiff’s PII where the plaintiff does not allege the existence of a “market” for the data that has been compromised or any other explanation for how the value of such data could have decreased because of its disclosure. *Rudolph*, 2019 WL 2023713, at *7–8. For example, in *In re GEICO Customer Data Breach Litigation*, the district court found that the alleged “loss in value of [plaintiffs’] personal data” was not an Article III injury in fact because the plaintiffs had “not allege[d] that they attempted to sell their personal information and were forced to accept a decreased price,” or “any details as to how their specific, personal information has been devalued because of the breach.” No. 21-cv-2210, 2023 WL 4778646, at *9 n.11 (E.D.N.Y. July 21, 2023) (“*GEICO*”), *report and recommendation adopted*, 691 F. Supp. 3d 624 (E.D.N.Y. 2023). Similarly, in *Cooper*, 2022 WL 170622, at *5, the district court found that allegations that the

plaintiff's PII diminished in value did not constitute an injury in fact where the plaintiff did not "plausibly allege that he intended to sell his personal information to someone else" or "that someone else would have bought it as a stand-alone product."

Here, as in *Rudolph*, *GEICO*, and *Cooper*, Cantinieri does not allege that there is a market for her PII, that she attempted to sell her PII, or that she was forced to accept a decreased price, or any other facts that could explain how the value of her data decreased as a result of its disclosure to unauthorized third parties. *GEICO*, 2023 WL 4778646, at *9 n.11; *Cooper*, 2022 WL 170622, at *5; *Rudolph*, 2019 WL 2023713, at *7–8. Accordingly, Cantinieri has not plausibly alleged that any diminution of her PII constitutes an injury in fact that could support her Article III standing to bring claims for damages and injunctive and declaratory relief.

V. Risk of Future Identity Theft and Fraud

The Amended Complaint alleges that Cantinieri faces an "increased risk of future identity theft and financial fraud posed by ill-intentioned unauthorized entities or criminals possessing [her] PII" and "the continued risk to [her] PII which remains in the possession of Defendants and is subject to further data breaches so long as Defendants fail to undertake appropriate and adequate cybersecurity measures." (Am. Compl. ¶ 99.) While Cantinieri can establish the first *McMorris* factor—that her PII was disclosed to a third party in a targeted attack—she cannot establish the other two factors—misuse of some exposed data and the high-risk nature of the exposed PII. Cantinieri thus fails to show a substantial risk of future identity theft under the *McMorris* factors. *See Cooper*, 2022 WL 170622, at *3 (finding that the plaintiff could not establish standing based on a future risk of identity theft where the plaintiff could only establish the first of the three *McMorris* factors).

a. McMorris Factor 1 — Targeted Attack

The first of the *McMorris* factors, “whether the data was compromised as the result of a targeted attack intended to get PII,” is the “most important factor.” *Bohnak*, 79 F.4th at 288. “Where a malicious third party has intentionally targeted a defendant’s system and has stolen a plaintiff’s data stored on that system, courts are more willing to find a likelihood of future identity theft or fraud sufficient to confer standing.” *Id.*; *see id.* at 288–89 (finding a substantial risk of future harm due to exposure of her PII where the plaintiff alleged that her PII was exposed when “an unauthorized actor [i.e., a hacker] leveraged a vulnerability in a third party’s software”); *cf. McMorris*, 95 F.3d at 303 (finding that the plaintiff failed to show a substantial risk of future identify theft where their PII was disclosed “inadvertent[ly] . . . due to an errant email sent to approximately 65 employees”).

The first *McMorris* factor is satisfied in this case because Cantinieri’s PII, including her date of birth, address, and license number, were “compromised as the result of a targeted attack intended to get PII.” *Bohnak*, 79 F.4th at 288; *McMorris*, 95 F.3d at 303. The Amended Complaint alleges that this security incident was a “targeted breach” of the ExpressNet portal by “unauthorized entities or cybercriminals.” (Am. Compl. ¶ 1.)

Although Defendants have put forward evidence contradicting the scope of the security incident, that evidence does not contradict the allegation that this security breach was “targeted” or enacted by “unauthorized entities or cybercriminals.” (*Id.*) Indeed, Defendants’ evidence shows that the PII disclosure occurred when an unauthorized entity posed as a legitimate insurance company and filed an application for an ExpressNet portal mimicking that company. (Disclosure Ltr.; Defs.’ Resp. to Pl.’s Interrog. No. 18, Defs.’ Mem. Ex. 1 at 6–7; CrowdStrike Exec. Summ.) The entity then used that fraudulent account to request and procure individual

motor vehicle records, including New York state motor vehicle records, which contain some PII. (See Cantinieri's MVR.)

b. McMorris Factor 2 — Misuse of Some Exposed Data

The second *McMorris* factor, whether some portion of the exposed dataset has already been misused, will support a finding that a plaintiff is at a substantial risk of identity theft or fraud, but is not required. *Bohnak*, 79 F.4th at 288. “For example, fraudulent charges to the credit cards of *other* customers impacted by the same data breach, or evidence that a plaintiff's PII is available for sale on the Dark Web, can support a finding that a plaintiff is at a substantial risk of identity theft or fraud.” *Id.*

Cantinieri cannot establish the second *McMorris* factor for the same reasons that she cannot show that she suffered from any actual or imminent injury from the disclosure of her PII. *See supra* Discussion I.

First, as previously discussed, Cantinieri fails to establish that fraudulent loan applications submitted in her name before August 2021 resulted from the disclosure of her PII through the ExpressNet portal because these incidents occurred *before* her PII was disclosed on September 23, 2021. *See supra* Discussion I; *see also* Defs.' Supp. Resp. to Pl.'s Interrog. No. 17, Defs.' Mot. Ex. 1 at 4–5; Defs.' Resp. to Pl.'s Interrog. No. 19, Defs.' Mot. Ex. 1 at 7–8.

Second, although the Amended Complaint alleges one fraudulent loan application submitted in Cantinieri's name *after* the September 23, 2021 disclosure—one that took place around June 10, 2022) (Am. Compl. ¶ 129)—Cantinieri has not established that this incident was causally related to the disclosure of her PII. *See supra* Discussion I.

Third, Cantinieri has failed to establish that the ExpressNet portal's security incident caused her to receive an increase in phishing emails and calls by entities seeking to engage in

fraud, even if these emails and calls could be considered “misuse” of her data.¹¹ As discussed, Cantinieri has not established that any of her phone numbers or email addresses were disclosed through the ExpressNet portal during the security incident. *See supra* Discussion 1; *see also* Defs.’ Supp. Resp. to Pl.’s Interrog. No. 17, Defs.’ Mot. Ex. 1 at 4–5; Defs.’ Resp. to Pl.’s Interrog. No. 19, Defs.’ Mot. Ex. 1 at 7–8. Thus, Cantinieri has failed to prove by a preponderance of the evidence that these emails and calls occurred because of Defendants’ disclosure of her PII.

c. McMorris Factor 3 — Nature of the Exposed PII

The third *McMorris* factor concerns “whether the exposed PII is of the type more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed.” *Bohnak*, 79 F.4th at 288. For example, the Second Circuit has found that “the dissemination of high-risk information such as SSNs especially when accompanied by victims’ names—makes it more likely that those victims will be subject to future identity theft or fraud.” *Id.* The Second Circuit has considered other types of PII to be less likely to subject plaintiffs to a risk of identity theft, such as PII that was already publicly available or that can be “rendered useless”—“like a credit card number unaccompanied by other PII.” *Id.*

As previously discussed, Defendants have demonstrated that Cantinieri’s SSN was *not* disclosed through the ExpressNet portal in the security incident, and Cantinieri has not proven otherwise by a preponderance of the evidence. *See supra* Discussion I. Defendants have demonstrated that only the following PII about Cantinieri was disclosed: her first and last name,

¹¹ *See In re Canon U.S.A. Data Breach Litig.*, No. 20-cv-6239, 2022 WL 22248656, at *5 n.4 (E.D.N.Y. Mar. 15, 2022) (finding that even though alleged unsolicited calls or emails due to the disclosure of a plaintiff’s PII may not constitute an injury in fact, these allegations could still “help satisfy the second *McMorris* factor”).

address, driver's license number, date of birth, and description (including gender, height, and eye color). (Cantinieri's MVR.)

Cantinieri argues that the disclosure of the type of PII at issue in this case poses a "high risk of identity theft or fraud." (Pl.'s Opp'n at 9.) This argument is unpersuasive. Cantinieri has not established that the disclosure of her driver's license number, name, address, date of birth, and description, unaccompanied by an SSN, would be likely to subject a person to a perpetual risk of identity theft or fraud. *See Bohnak*, 79 F.4th at 288; *see also Liau*, 2024 WL 729259, at *5 (finding that plaintiffs failed to establish the third *McMorris* factor where "plaintiffs have not plausibly alleged why the leak of the data at issue"—names, addresses, and phone numbers, but not payment data or passwords—"would causally lead to identity theft").¹²

Although Cantinieri relies on *In re USAA Data Security Litigation*, 621 F. Supp. 3d 454 (S.D.N.Y. 2022), (Pl.'s Opp'n at 9), that case is distinguishable. In *USAA Data Security*, the court found that the disclosure of an individual's driver's license number was likely to pose a risk of future of identity theft and fraud because the complaint plausibly alleged that "drivers' license numbers, in addition to other personal information already gathered from other sources, can provide an opening for fraud, including applying for credit cards or loans or opening bank accounts." *Id.* at 466–67. The court acknowledged that courts in other cases had found that the disclosure of a driver's license number without more sensitive data did not generate a risk of identity theft. *Id.* at 467 n.5. But the court found that, unlike those cases, the complaint had well-pleaded "allegations of actual proof of identity theft as a result of the disclosure." *Id.* Here, the

¹² Cantinieri argues that the specific types of PII disclosed in this case "are a critical part of building fraudulent identities" but does not explain how or support this argument with allegations in the Amended Complaint or evidence in the record. (Pl.'s Opp'n at 9.)

Amended Complaint lacks allegations that the disclosure of a driver's license number, name, address, and birthdate, can provide "an opening for fraud" even when no SSN has been disclosed. Moreover, unlike in *USAA Data Security*, Cantinieri has failed to establish *actual identity theft* resulting from the disclosure in this case. *See supra* Discussion I; *cf. USAA Data Security*, 621 F. Supp. at 466–67 & n.5. Similarly, in *Rand*, the court found that the plaintiff plausibly alleged that the disclosure of a driver's license number is likely to result in identity theft where it alleged that the number was "used to file fraudulent unemployment claims, open a new account, take out a loan, or commit income tax refund fraud." 637 F. Supp. 3d at 67. The Amended Complaint in this action makes no similar allegations.

VI. Injuries Based on the Risk of Future Identity Theft or Fraud

The Amended Complaint alleges that Cantinieri has incurred "costs associated with the . . . *prevention* of identity theft and financial fraud." (Am. Compl. ¶ 7 (emphasis added).) It alleges that Cantinieri has been unable to "conduct ordinary consumer transactions" because she froze her credit card due to the "ongoing threat of future acts of identity theft." (*Id.* ¶ 128.) The Amended Complaint also alleges "emotional anguish and distress, including, but not limited to fear and anxiety related to the exposure and exploitation of her PII and resulting vulnerability to imminent and impending identity theft or financial fraud in the future." (*Id.* ¶ 17.) Because Cantinieri has not established a substantial risk of future identify theft of fraud, *see supra* Discussion I, the costs she incurred to mitigate against a speculative risk of future injury cannot confer standing in this case. *See McMorris*, 995 F.3d at 303 (finding that where plaintiffs "have

not alleged a substantial risk of future identity theft,” however, “the time they spent protecting themselves against this speculative threat cannot create an injury”).¹³

VII. Failure to State a Claim

Because Cantinieri cannot establish standing for any of her claims,¹⁴ this Court does not have jurisdiction over this action and the case must be dismissed. *Soule*, 90 F.4th at 45; U.S. Const. art. III § 2; Fed. R. Civ. P. 12(b)(1). Thus, I do not reach Defendants’ arguments that the Amended Complaint fails to state any claim upon which relief can be granted under Rule 12(b)(6).

CONCLUSION

For the reasons stated above, Cantinieri has failed to establish that she has standing under Article III of the U.S. Constitution to bring any of the claims asserted in the Amended Complaint. Accordingly, Defendants’ Motion to Dismiss the Amended Complaint (ECF No. 79)

¹³ Further, to the extent that the Amended Complaint alleges “emotional anguish and distress” as a result of the disclosure itself, such a “perfunctory allegation” without any allegations explaining why the disclosure would cause such distress, “is insufficient to plausibly allege constitutional standing.” *Maddox v. Bank of New York Mellon Tr. Co., N.A.*, 19 F.4th 58, 66 (2d Cir. 2021); *see also In re GEICO*, 2023 WL 4778646, at *9 n.11 (finding general allegations of “anxiety” and “emotional distress” due to defendant’s misconduct insufficient to support standing because plaintiffs failed to offer any “reason why (or how) the disclosure of their data has caused them such distress”), *report and recommendation adopted*, 691 F. Supp. 3d 624 (E.D.N.Y. 2023).

¹⁴ Cantinieri also argues that the injuries alleged in the Amended Complaint satisfy the “redressability” requirement of Article III. (Pl.’s Opp’n at 11.) Because I have found that Cantinieri’s alleged injuries either fail to meet the injury in fact and/or traceability requirements of Article III, *see supra* Discussion I, I need not reach the redressability requirement.

is granted, and the Amended Complaint (ECF No. 72) is dismissed without prejudice pursuant to Rule 12(b)(1), Fed. R. Civ. P.

Dated: Central Islip, New York
December 23, 2024

/s/ Nusrat J. Choudhury
NUSRAT J. CHOUDHURY
United States District Judge